UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/567,752	02/10/2006	Paolo Abeni	09952.0022	5634

22852 7590 06/23/2010

FINNEGAN, HENDERSON, FARABOW, GARRETT & DUNNER LLP
901 NEW YORK AVENUE, NW
WASHINGTON, DC 20001-4413

EXAMINER	
SIMS, JING F	

ART UNIT	PAPER NUMBER
2437	

MAIL DATE	DELIVERY MODE
06/23/2010	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/567,752	ABENI, PAOLO	
	Examiner	Art Unit	
	JING SIMS	2437	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *28 April 2010*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☐ Claim(s) *1-50* is/are pending in the application.

4a) Of the above claim(s) *1-25* is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *26-50* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 04/08/2010 has been entered.

2. Claims 26 and 50 are amended. Claims 1-25 have been canceled.

3. The objection to Specification is withdrawn in view of Applicant's amendments.

4. The 35 U.S.C. §101 rejection over claims 26 and 50 are withdrawn in view of Applicant's amendments.

Claim Rejections - 35 USC § 112

5. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

6. Claim 26 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which the Applicant regards as the invention.

Claim 26 recites the limitation "said data" on page 2, line 3 from bottom. It is not clear the antecedent basis for this limitation is "captured data" or "response data". Claim 26 also recites the limitation "attack and response signatures". It is indefinite whether this "attack and response signatures" are the same signatures of "at least one

attack signature" on page 2 and lines 15-16 or "response signatures" on page 2 and lines 4 from the bottom. the claimed feature of "comparing with response signatures response data being transmitted on said network as a response to said data marched with said at least one attack signature" is indefinite because it is not clear whether it should be interpreted as comparing response signatures with response data or any other interpretations.

Response to Arguments

8. Applicant's arguments, see page 10-16 of Remarks, filed 04/28/2010, with respect to the rejection(s) of claim(s) 26, 38, 30, 42, 31, 43, 35, 47, 36, 48, 39, 49, 26, 38, 29, and 41 under *35 USC § 102 and 35 USC §103* have been fully considered and are persuasive. Therefore, the rejection has been withdrawn. However, upon further consideration, a new ground(s) of rejection is made in view of Dettinger et al (US 2004/0073810 A1, Cole et al (US 2004/0015728 A1) and Moharram (US 7,246,376 B2)

Claim Rejections - 35 USC § 103

9. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

10. **Claims 26-29, 38-40 and 50 are rejected under 35 U.S.C. 103(a) as being unpatentable over Lahtinen (European Publication no. EP 1330095 A1), in view of Dettinger et al (US 2004/0073810 A1, hereinafter Dettinger)**.

Lahtinen discloses:

As per claim 26, **an intrusion detection system** *(i.e. [0013], a flow monitoring mechanism enhancing system)*, for detecting unauthorised use of a network, comprising:

at least one **computer** *(i.e. page 10, [0069], the system implemented in a computer cluster)*; and

a non-transitory computer readable medium encoded with a computer program product loadable into a memory of the at least one computer the computer program product *(page 12, claim 21, a computer program product stored on a computer readable storage medium)* including:

instructions for **a sniffer** *(i.e. [0014], lines 31-33, the system for the monitoring process; or fig. 2, block 220 host ID recognition block and/or block 222 client ID recognition, [0030], and [0031] lines 18)*, for **capturing data** *(i.e. [0014], lines 31-33, identifying at least one response descriptor)* **being transmitted on said network** *(i.e. [0014], lines 32 and 34, data stream traveling from the server to the client, and traveling from the client to the sever)*;

instructions for **a pattern matching engine** *(i.e. fig. 2, block 230, finger print matcher block, and [0031], lines 18-20, fingerprint matcher block)*, **for receiving data captured by said sniffer** *(i.e. [0031] lines 18, if the corresponding entry is not found,*

they forward the data stream to a fingerprint matcher block) and **comparing said the captured data with attack signatures** *(i.e. [0031] lines 18, checks whether the HTTP data stream contains parts resembling known attack patterns, i.e. known fingerprints)* for **generating an event** *(fig. 6, block 616, event classification)* when a **match between the captured data and at least one attack signature is found** *([0060], lines 1-3, if the result of the comparison is that the known misuse pattern are detected)*.

Lahtinen does not discloses instructions for response analysis engine triggered by said event, for comparing with response signatures response data being transmitted on said network as a response to said data matched with said at least one attack signature and for correlating results of said comparisons with attack and response signatures for generating an alarm.

Dettinger also discloses **comparing the captured data with attack signatures for generating an event when a match between the captured data and at least on attack signature is found** (i.e. [0066], lines sample or identify a viral indicator associated with the metafile; wherein sampling or identifying corresponding with comparing, metafile corresponding with captured data; viral indicator corresponding with attack signatures; and compare the sample viral indicator against profile criteria accessed from a database 69, this comparison is to further identify a attack signature; should match is found).

Dettinger further discloses:

instructions for a **response analysis engine triggered by said event for comparing with response signatures** *([0066], lines 13-16, and [0068]: correlated field*

of the database 69 corresponding with response signatures) **response data being transmitted on said network as a response to said data matched with said at least one attack signature** *([0066], lines 13-16: risk level corresponding with response data, see also fig. 6)* and **for correlating results** *([0068], and fig. 6, 262: assign risk level)* **of said comparisons with attack and response signatures for generating an alarm** *(fig. 6, 264, route to user; see also [0068], lines 7-10, programmatically associate with the data and displayed to the user)*.

Lahtinen and Dettinger are analogous art because they are from the same field of endeavor of detecting malicious activity on networks.

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify an malicious pattern transmitted on a network as described by Lahtinen, also Dettinger and add further analyzing the risk level of the malicious pattern as taught by Dettinger because it would minimizes harm caused by viral infections in a manner that addresses above (such as the description in paragraph [0006]: continually anticipate new viruses by updating and refocusing protective code; and see also paragraphs [0005] and [0007]) (see Dettinger, page 2, [0016]).

As per claim 27, the system of claim 26 is incorporated and Lahtinen discloses:

wherein said response data is captured by said sniffer by performing an analysis of source IP address in data packets transmitted on said network *(i.e. page 3, [0009], IP frame on TCP packets, target and destination port, for example)*.

As per claim 28, the system of claim 26 is incorporated and Lahtinen discloses:

wherein said response data is captured by said sniffer by performing an analysis of both source and destination IP addresses in data packets transmitted on said network *(i.e. page 3, [0009], IP frame on TCP packets, target and destination port, for example)*.

As per claim 50, a non-transitory computer readable medium encoded with a computer program product loadable into a memory of at least one computer, the computer program product including software code portions for performing the method of any one of claims 38 to 49 *(i.e. NIDS runs on a server)*.

Claims 38, 39, and 40 are method claims corresponding to the system claims 26, 27, and 28, therefore are rejected under the same reasons set forth in the rejections for claims 26, 27, and 28.

11. **Claims 29 and 41 are rejected under 35 U.S.C. 103(a) as being unpatentable over Lahtinen in view of Dettinger, and further in view of Yadav (US patent publication no. 2003/0149888 A1)**.

As per claim 29, Lahtinen in view of Dettinger discloses they system of claim 26;

However, Lahtinen does not explicitly discloses said response data is captured by said sniffer by analysing transport level information in data packets transmitted on said network;

Yadav discloses data packets have been transmitted on transport level *(i.e. page 3, [0034], an IDS may be implemented on network transport layer so incoming packets may be monitored)*.

Lahtinen, Dettinger and Yadav are analogous art because they are from the same field of endeavor of intrusion detection system by pattern matching.

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the packets transition as described by Lahtinen and specify the packets are transmitted on transport layer as taught by Yadav because it would provide a standard way of packets exchanges at the time the invention was made.

Claim 41 is method claim corresponding to the system claim 29, therefore are rejected under the same reasons set forth in the rejections for claim 29.

12. **Claims 30 and 42 are rejected under 35 U.S.C. 103(a) as being unpatentable over Lahtinen, in view of Dettinger, and further in view of Goldstone (US 7,301,899 B2)**.

As per claim 30, Lahtinen in view of Dettinger discloses the system of claim 26, however, they do not discloses said response analysis engine generates the alarm when said response data indicates that a new network connection has been established.

Goldstone discloses wherein said response analysis engine generates the alarm when said response data indicates that a new network connection has been established *(i.e. col. 2, lines 58-60)*.

Lahtinen, Dettinger, and Goldstone are analogous art because they are from the same field of endeavor of detecting malicious activity on networks.

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify an malicious pattern transmitted on a network as described by Lahtinen in view of Dettinger and add further detecting a new connection as alarming situation as taught by Goldstone because it would provide positive steps in preventing or at least diminishing the potentially devastating effects of a DOS attack (see Goldstone, col. 4, lines 13-15).

Claim 42 is method claim corresponding to the system claim 30, therefore are rejected under the same reasons set forth in the rejections for claim 30.

13. **Claims 31 and 43 are rejected under 35 U.S.C. 103(a) as being unpatentable over Lahtinen, in view of Dettinger, and further in view of Cole et al. (US 2004/0015728 A1, hereinafter Cole)**.

As per claim 31, Lahtinen in view of Dettinger discloses the system of claim 26, however, they do not discloses wherein said response signatures are arranged in two categories, response signatures identifying an illicit traffic, and response signatures identifying legitimate traffic.

Cole discloses wherein said response signatures are arranged in two categories, response signatures identifying an illicit traffic, and response signatures identifying legitimate traffic *(i.e. [0361], high risk vulnerability level scale corresponding with illicit traffic, and low risk vulnerability level scale corresponding with legitimate traffic)*.

Lahtinen, Dettinger, and Cole are analogous art because they are from the same field of endeavor of detecting malicious activity on networks.

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify a risk level as described by Dettinger in paragraph [0066] and add what the level categories are as taught by Cole because it would provide traditional vulnerability scale which easy and reasonable categorizing the risk levels (see Cole, [0360]).

As per claim 32, the system of claim 31 is incorporated, and Dettinger discloses:

wherein said response analysis engine generates the alarm when a match between the response_data and a response signature identifying illicit traffic is found *(fig. 6, block 618 create alert; and [0060], lines 4-5, an alert is generated)*.

Claim 43 and 44 are method claims corresponding to the system claims 31 and 32, therefore are rejected under the same reasons set forth in the rejections for claims 31 and 32.

14. **Claims 33, 34, 45, and 46 are rejected under 35 U.S.C. 103(a) as being unpatentable over Lahtinen, in view of Dettinger, further in view of Cole, and further in view of Moharram (US 7,246,376 B2)**.

As per claim 33, Lahtinen in view of Dettinger, further in view of Cole discloses the system of claim 31;

Lahtinen, Dettinger, and Cole do not disclose said response analysis engine comprises a counter which is incremented when a match between the response data and a response signature identifying legitimate traffic is found;

Moharram discloses a counter which is incremented when a match between the response data and a response signature identifying legitimate traffic is found *(i.e. col. 4, lines 13-16; and col. 5, claim 1, lines 48-53)*.

Lahtinen, Dettinger, Cole, and Moharram are analogous art because they are from the same field of endeavor of detecting malicious activity on networks.

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the packets transition as described by Lahtinen and add counter as taught by Maher because it would provide possibility of fine control over an objective subject.

As per claim 34, Moharram discloses when said counter reaches a predetermined value, said response analysis engine terminates without generating any alarm *(i.e. col. 5, claim 1)*.

Claims 45 and 46 are method claims corresponding to the system claims 33, and 34, therefore are rejected under the same reasons set forth in the rejections for claims 33 and 34.

15. **Claims 35-37 and 47-49 are rejected under 35 U.S.C. 103(a) as being unpatentable over Lahtinen, in view of Dettinger, further in view of Moharram (US 7,246,376 B2)**.

As per claim 35, Lahtinen in view of Dettinger discloses the system of claim 26. They do not disclose wherein said response analysis engine comprises a time-out system triggered by said event for starting a probing task.

Moharram discloses wherein said response analysis engine comprises a time-out system triggered by said event for starting a probing task *(i.e. col. 5, claim 1, see also Fig. 3, lines 5-35)*.

As per claim 36, the system of claim 35 is incorporated.

Moharram discloses:

wherein said probing task verifies if any data has been detected on said network as the response to said data matched with said at least one attack signature and, if such condition is verified:

generates the alarm in case only response signatures indicating legitimate traffic have been used by said response analysis engine *(i.e. col. 5, claim 1, lines 48-53)*; or

ends the probing task in case only response signatures indicating illicit traffic or both response signatures indicating legitimate traffic and illicit traffic have been used by said response analysis engine *(i.e. col. 5, claim 1)*.

As per claim 37, the system of claim 36 is incorporated, and Lahtinen discloses:

wherein, if such condition is not verified, said probing task attempts to perform a connection to a suspected attacked computer, for generating the alarm if such attempt is successful, or for ending the probing task if such attempt is unsuccessful *(i.e. fig 1B, and [0009])*.

Claim 47-49 are method claims corresponding to the system claims 35-37, therefore are rejected under the same reasons set forth in the rejections for claims 35-37.

Examiner Notes

16. Examiner has pointed out particular references contained in the prior arts of record and in the body of this action for the convenience of the applicant. Although the specified citations are representative of the teachings in the art and are applied to the specific limitations within the individual claim, other passages and figures may apply as well. Applicant should consider the entire prior art as applicable to the limitations of the claims. It is respectfully requested from the applicant, in preparing for response, to consider fully the entire reference as potentially teaching all or part of the claimed invention, as well as the context of the passage as taught by the prior arts or disclosed by the Examiner.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to JING SIMS whose telephone number is (571)270-7315. The examiner can normally be reached on 9:00am-5:00pm EST, Mon-Thu.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571)272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/JING SIMS/
Examiner, Art Unit 2437

/Matthew B Smithers/
Primary Examiner, Art Unit 2437